Meta

EU Youth Privacy Forum

Building blocks for age-appropriate digital services – a closer look at age assurance and age verification

18 January 2023
Brussels, Belgium

High-level summary

A combination of informative keynote presentations and interactive breakout sessions enabled the EU Youth Privacy Forum to develop a broad understanding of age-appropriate digital services and contribute to an active panel discussion. Conclusions drawn included recognition that there are a myriad of building blocks that can make digital services age-appropriate (including, but not limited to, age assurance) and that there must be flexibility in how these building blocks are used to allow practical application in different services and at a global scale.

Also to be considered at a global scale, are the challenges of age assurance including consideration of the various equities when determining appropriate age assurance method(s) in context, such as seriousness and likelihood of risks, proportionality, efficacy, inclusiveness, data minimisation, balance with children's fundamental rights and freedoms, usability and cost. In addition, there was agreement that international standards (on those equities that could be measured) would help avoid a patchwork approach to regulation and support policy decisions for different use cases. State level electronic identity systems could form an additional choice for users to verify their age on digital services, however they would not be a 'silver-bullet', with the same equities still needing to be factored in.

01 Background

The Meta EU Youth Privacy Forum launched in June 2022, bringing together stakeholders with an interest in youth issues to discuss key challenges and exchange views on topical privacy and safety policy issues relating to the protection of young people online. Meta recognised the importance of a multi-stakeholder approach and created this dedicated Forum where industry, regulators, academics, trades and NGOs are invited to share their perspectives, broadening one another's understanding on complex youth topics and shared objectives, and to work together to find constructive solutions and bridge gaps.

The series to date has run as regional and thematic workshops where attendees have explored the European youth regulatory landscape and key policy challenges for keeping young people safe online, whilst having privacy equities in mind. At Meta's October Forum event, participants took a deep-dive on the European Commision's Regulation Proposal on preventing and combatting child sexual abuse, hearing from experts about different approaches to prevention, including technological solutions, psychological treatment, and possible government and legal approaches.

Meta's third Youth Forum took place in January 2023, a week after the European Commission concluded its calls for applications from interested parties to work on the EU code on age-appropriate design (as set out in its Better Internet for Kids Strategy), the day before UK regulators and key stakeholders met in London to workshop the measurement of specific aspects of age assurance methods, and as policymakers returned to their offices to commence work on their 2023 roadmaps, including developing and piloting state level digital identity systems, amongst many other things. Protecting young people online remains a priority for privacy and safety stakeholders at all levels and it is clear that conversations and debate on the best way to achieve this are set to continue throughout 2023 and beyond.

The January Youth Forum took place in Brussels and focused on the building blocks for age-appropriate design. This report will focus on the discussions that took place during that event. Respecting Chatham House Rule, names have not been attributed to individual comments beyond the Meta facilitators.

02 Introductory Remarks

Participants at the Forum were welcomed by four Meta Directors: Cecilia Alvarez and Marco Pancini (EMEA Privacy Policy), David Miles (EMEA Safety Policy) and Marisa Jimenez Martín (EU Affairs).

Meta welcomed attendees to the third event in the Forum series and acknowledged both those that were returning, having joined at previous events, but also the growing network of stakeholders joining for the first time, hoping for continued engagement as the series continues. A recap of the previous Youth Forum events was made, which evidenced the benefits that diversity of attendees has to rich discussions, representing a range of sectors and interests, with the shared objective of keeping young people safe online. Indeed, Meta's Youth Forum purpose is to give the privacy and safety communities the opportunity to share their views and contribute to discussions which require multi-stakeholder engagement.

03 A framing discussion on the building blocks for age-appropriate digital services

Meta Privacy and Safety EMEA Leads introduced the first session of the afternoon, giving the context that young people have the right to participate in the digital world, to develop skills and experiences as digital citizens and be empowered to use their voices for good, as acknowledged in the UN Convention on the Rights of the Child. Protecting and empowering all users online should be of great importance to industry and policymakers alike, however specific protections should also be implemented in the best interests of young people, taking into account the role that parents play, and facilitating age-appropriate experiences that strike a balance between protecting young people and facilitating their connection and development in the digital environment.

It was explained that, for Meta, joint consideration of the privacy, safety, and wellbeing of young people on Meta's platforms is essential to address an age-appropriate experience, and Meta continues to make ongoing investments in this space. Meta has developed over 30 privacy, safety and wellbeing tools and protections under this holistic approach for young people and their families, and the Forum was shown a short video which highlighted just a few of these, including default settings, content moderation, protection from unwanted interactions and parental supervision tools. These examples illustrate some building blocks for age-appropriate digital services intended to provide food for thought for this first break-out session.

Sat in small groups, attendees were asked to consider the building blocks that can support age-appropriate experiences on digital services and the roles that different stakeholders might play in supporting them. After discussing in break-out groups, each appointed a rapporteur to share their discussions with the wider Forum.

On the question of 'what makes an online service age-appropriate', groups explored what 'age-appropriate' actually meant. Many shared that this can be hard to define but generally involves an understanding of the audience using the specific digital service and then, the likelihood and seriousness of risks associated thereto. One group described that an age-appropriate online service was one focused on a 'safe, private and tailored experience' for someone of a particular age, but others expressed the need for inbuilt flexibility to accommodate the growth and developmental stages of the young person, and allowing for individual variances in cultural or societal attributes.

Another group spoke about the ‘4Cs’, as set out in a paper by Sonia Livingston and Mariya Stoilova - content, contact, conduct and contract. These 4Cs relate to the different risk categories in the digital environment and can help industry and policymakers in devising relevant building blocks to mitigate or reduce risks. This point was expanded to recognise that the risk assessment is more clear when legal requirements exist as to what content or experiences are prohibited for young people - at times with ages ranging across the regions, for example, prohibiting access to violent and pornographic content, age-gated movies/ videogames following age classification standards or advertisements around alcohol, tobacco or products high in fat, sugar or salt. There are learnings from the media industry to be considered regarding age classification standards, which are not necessarily that useful when content is user generated.

Groups considered where building blocks may go beyond industry responsibility, for example the role of parents and guardians, but also educators. Parents will often play a role in determining what they believe is age-appropriate for their children and inherent in this is their understanding of the risks, opportunities and safeguards that exist. When considering the point on flexibility, groups highlighted the differing family structures but also variances in cultural norms around dialogue between parents and young people and expectations around parental control.

Groups also started to explore the semantics around the terms ‘age assurance’, ‘age verification’, and ‘age estimation’. With the assistance from attendees who have been involved in developing definitions for these terms, it was agreed that there is benefit in defining these terms globally to ensure clarity. Attendees suggested that ‘age assurance’ was the umbrella term referring to the process of establishing or understanding the age of an individual; age assurance is a collective term that covers both age verification and age estimation. ‘Age verification’ is the determination of an individual’s age. ‘Age estimation’ is the process of assessing that a user is likely to fall within an age range, or is over or under a stated age. Age estimation can become more accurate as technology advances and access to suitable databases improve. These discussions paved the way for the first keynote presentation.

04 Keynote presentation on age assurance, age verification and standardisation

Sharing a keynote presentation, the Forum benefitted from an overview of the challenges involved with digital age assurance from a reputed expert on age-check systems and standardisation.

The speaker gave examples of how they might assure someone as to how old they are and, if needed, that they are who they say they are. In person this may be done by a visual check - do they look like an adult? Are they someone you have worked with previously, or if not, do you trust that the third party who has invited them to speak is confident in who they say they are? Do they have any documentation on them that matches who they claim to be, or how old they are? - a credit card, a driving licence, a passport. A credit card gives some assurance - the card issuer is a reputable company and they will have done thorough checks. A driving licence goes a step further and includes a photo for comparison. However, it also includes their date of birth and address. The licence will have been issued by a government agency and so should be more reliable. A passport goes even further, it tells you where they were born, it has to be renewed at regular intervals so that the government can re attest that they are who they say they are.

However, these are not foolproof. The speaker gave the example that in some parts of the world, some 40% of driving licences had an identical licence number, elsewhere several licences have been issued for a ‘Mr. M. Mouse’. There is also the challenge of translating these checks to the digital world where official documents can easily be spoofed. We are living in an increasingly digitised world and babies born today may never possess a physical driving licence, so this is a challenge society needs to be considering now.

The speaker highlighted that assurance can exist as identity assurance but also, separately, age assurance. Within each, there are degrees, or levels, of assurance. When determining which level to use, you need to think about why you need the assurance, what is the purpose for checking, how much assurance do you need? For example, the level of assurance needed by Meta to verify someone's identity to ask to speak at an event is very different when compared with a bank verifying identity for the purposes of providing a mortgage.

Industry, regulators and parents need to think about the different use cases and proportionality. There are tradeoffs to be considered: friction and ease of use, protection of children from harm, empowering young people to develop and access age-appropriate things, balancing rights and freedoms. The speaker shared that they could not endorse a particular approach. There is no one-size-fits-all, no silver-bullet approach. This is why guardrails are needed. Something that industry and regulators can refer to that are at an international level and mean the same thing to different people in different places. This is where standardisation comes in.

The speaker gave an overview of the work currently being done on the standardisation of age assurance under ISO 27566, which at the time of the Forum had just been voted on as a project internationally with 100% backing to proceed. This draft standard comes in two parts, the first being a framework that describes the characteristics of the level of assurance and the second is on how to test it. The overarching aim is to have something that can be used to enable policy decisions. The speaker also spoke about standard IEEE 2089-2021 which sets out processes by which organisations seek to make their services age-appropriate, including exploring how age verification can be deployed as part of an age-appropriate environment.

05 An exploration of age assurance and age verification

Objectives, methods and key considerations

The keynote provided a helpful ‘scene setter’ for the second break-out discussion. As Forum attendees had discussed in the first break-out session, age assurance can be one of the building blocks used to support age-appropriate experiences on digital services. However, understanding a user's age is a complex, industry-wide challenge that requires thoughtful solutions to appropriately balance the different equities.

Meta gave context about the challenges and inequities, particularly when operating at a global level; societal issues such as understanding a user’s age are seen in the global north but are also relevant, and the challenges possibly exacerbated, for the global south. From research, it is understood that in South Africa, 60% of children do not live in two parent families. For inclusivity purposes, there is a huge need to find solutions that work at a global scale, taking into account the best interests of the child and the different family structures that exist.

To give insight into some of the age assurance methods currently on the market, Meta invited presentations from two age verification providers. Each spoke of the importance of proportionality and recognising that age assurance isn’t ‘KYC’ as required in sectors such as financial services - often it is not proportionate or necessary to verify the identity of the individual, you don’t need a sledgehammer to crack a nut. The role of age assurance solutions are to determine the age, age range, or that an individual is above or below a stated age. Its purpose is not to disclose or gather identity and it is technically possible to provide age assurance without doing so. The providers shared insight into the continuing innovation taking place within the industry, sharing their respective approaches and considerations including using images, voice and text to provide levels of assurance as to the age of a user.

Inspired by the presentations, Youth Forum participants broke into smaller groups to expand on the list of currently available age assurance methods, discussing the levels of assurance they provide and whether they amount to age verification or estimation. There was a good awareness of the range of solutions that could be deployed on digital services from self-declaration of age to ID verification, third party checks such as through a OS operator as well as from a utility or telecoms provider, to AI estimations based on face based prediction, an individual's voice or the size of their hand, signals from a user's interactions with others, or their interests. The list went on. It was clear that there are a variety of methods already available but also that each had further considerations or trade-offs that would need to be taken into account when deciding if it was the appropriate solution for the use case at hand.

The groups discussed the different equities at play - privacy, accuracy, proportionality, scalability, fairness, usability, risk of abuse/spoofing, and cost. Participants across the groups agreed that it was a case of balancing these equities to determine which level of assurance was appropriate. Industry needs to determine what data points are necessary for the level of assurance required, and question to what extent the available solutions provide the assurance needed for the audience it is being applied to.

A risk-based approach was discussed with reference made to 'fraud, friction and fees' and particularly in the case of young people, a consideration of risk of harm, both from a content and data processing perspective. However, risks were also cited in relation to obtaining and storing too much information, for example if data stored by a company for the purpose of assessing age is then subject to a data leak or hacking. The solutions need to be cognizant of not only protecting young people's experiences on the digital service, but also of their privacy.

The groups explored the different use cases where age assurance may be appropriate and why certain methods are more appropriate in specific situations.

Finally, the group considered how regulation or standardisation on this topic is driven. Technology is moving quickly and if legislators are too prescriptive, by the time new laws are passed they risk being outdated. New regulations must be evidence driven but also be flexible enough to allow for innovation to take place and for industry and parents to adapt to the needs of young people and their families, and considerations at a global scale. Principles based standards should be pursued at an international level, taking into account research and lessons learned from industry already working in this space. In addition, there is much that can be learnt from other industries that have been tackling these challenges in other sectors, at least regarding risks comparable to money laundering or terrorism, for example, financial services. As technology companies increasingly move into the Fintech space, there is a greater need to collaborate and learn from each other.

06 Could eID be the 'Silver Bullet' approach to age assurance for digital services? Or simply another age verification method?

A keynote presentation on the European Commission's proposal for the European Digital Identity ('EUDI') Wallet and expert panel discussion

The Forum welcomed a second keynote speaker who provided an overview of the European Commission's proposal for an EUDI Wallet. In 2020, the European Council called for the development of an EU-wide framework for secure public electronic identification. The ambition of the Commission is to create a universally usable Wallet, that all EU citizens may use on a free of charge, voluntary basis, and that users can take control of their identity, what attributes are visible and who they wish to share it with.

The EUDI Wallet would provide access to both public and private services. The proposal sets out that certain digital services would be obliged to offer use of the Wallet, including public sector services and Very Large Online Platforms (as defined in the Digital Services Act). Other private service providers may choose to include its use which would be promoted by codes of conduct.

The EUDI Wallet requires unique identification of a user. As part of the dataset, the Wallet will contain the birthdate of the user and will originate from authoritative sources. This could result in the Wallet being used for a number of technical purposes, for example confirming whether a user is over a predefined age. However, the minimum age whereby individuals could be required to have an identity card significantly differs per Member State.

There are four work strands for the development and testing of the EUDI Wallet with a roadmap to the end of 2023. In December 2022, the Transport, Telecommunications and Energy Council adopted the General Approach. The legislative process will continue into 2023 with expectations from the Commission that the proposal will be adopted by the end of the year. At the time of the Forum, development of a common toolbox was underway, including common standards and specifications to ensure best practice. Large-scale pilots for different use cases are expected to take place in Spring 2023, and the outcomes of these are to inform development and iterations of the common toolbox and framework. Finally, development of a reference application will commence and will be tested as part of the large-scale pilots. At the conclusion of the pilots, there might be a minimum viable product for the EUDI Wallet process.

A number of attendees had been involved in the work undertaken as part of the euCONSENT Project and shared that the Commission's EUDI work could benefit from several of the learnings from that project's small scale pilot when looking at building the larger scale pilots for these use cases, particularly if considering age assurance as a use case.

A question was also raised as to how the EUDI Wallet would be funded - whether it would come from taxpayers' money, or through commercial operators, and with this, a question about whether there would be a need to rely on tracking by trusted service providers. There is more to be done here by the Commission and in discussions at Member State level.

With Forum attendees having benefited from the keynote setting out the Commission's proposals, a number of questions were posed to an expert panel to consider whether the EUDI Wallet might be the 'silver-bullet' for age assurance on digital services.

It was agreed that the Commission's proposals could be used as a method for age assurance and could provide for an extremely reliable source. Experts felt it was great to see plans to empower EU citizens to access and use trusted digital identity. For a number of potential use cases, this option is likely to be extremely convenient, for example avoiding the need to carry hard copy identification or being able to access your digital identity from anywhere.

However, as Forum participants had discussed in earlier sessions, it is vital to consider the various equities and, in considering this potential use case, taking into account that the individuals to be age-assured would be children rather than adults. The experts stressed the importance of flexibility and choice for users - the EUDI Wallet could be one option in a list, however digital services should also seek to provide options for users where ID is not required. Giving the example of Meta's age verification Menu of Options test, one expert shared how when given the choice of ID upload or video selfie, 81% of people presented with the option chose to use Yoti's video selfie to verify their age over ID.

The panel considered some of the risks that may stem from a government owned tool. Whilst the EUDI Wallet proposed is not mandatory for citizens, it should not be ruled out that future leaders could make it so. Inherent in this are a number of risks including government surveillance as well as a single point of failure. Users, including young people, are becoming increasingly privacy conscious. Some users will be very mindful that they are linking their online personas to state identity systems. For many, online digital services are spaces where they can explore new interests or learn more about topics which they may not necessarily wish to be associated with, for example religion or sexuality. An example was given of someone who may be researching drugs as part of their homework - if they reached a site where they needed to give assurance as to their age, would they feel comfortable using their state issued Wallet to permit their access? Users can feel safer online if they feel confident that their activity is not being linked to their individual identity, whether through a state owned system or otherwise. The essence of age assurance is being able to prove age without disclosing who you are.

The experts also raised a challenge to the level of inclusivity, particularly for very young citizens. At what age would it be appropriate for someone to have a digital identity? Would their parents have control over when and where it could be used, at least whilst a child was of a younger age? The age for issuance for governmental identification differs across the EU and ranges from 12 to 18.

The euCONSENT project explored the technical feasibility for an interoperable solution where user experience was as smooth as possible, enabling a user to verify their age and move from one website to another without needing to repeat the process. That project demonstrated that it is possible to do this in a privacy preserving manner. The project also demonstrated the ability for different sectors and industries to come together to find solutions. Forum attendees stressed the importance of new initiatives taking into account the lessons learnt from previous pilots and recognising that industry has been innovating in this space for some time.

The panel summarised that, in answer to the question about whether eID could be the silver-bullet to age assurance, the EUDI Wallet does not alone solve the challenges that come with understanding user age on digital services. It may be, however, suitable as an additional option offered to users to verify their age in certain use cases and where a user is entitled to hold, and feels comfortable using, state issued ID. There is further work to be done to pilot the Wallet and the Commission is likely to benefit from engagement with industry to understand the lessons learnt from developments in this space so far.

07 Closing remarks

The Forum concluded with closing remarks. Meta shared their thanks with all those attending for sharing valuable expertise, giving insight into what needs to be addressed, and what can be expected in the digital identity and age assurance spaces in 2023 and beyond. These sessions are so valuable because they allow everyone to contribute and demonstrate the importance of having representatives from across different sectors, and from several European countries come together to discuss these topics, share regional differences and shared challenges and shape how these topics move forward.

After the event concluded, attendees were invited to join for a cocktail and further informal discussions whilst enjoying the evening view across Brussels from the venue's rooftop terrace.


Meta